IN THE CLAIMS:

1.   (Currently Amended)   A system for identifying a computer virus undesirable content in responses sent in reply to a user request for content, the system comprising:

a user input device that generates a request for content including an address of a target server, a destination header, a request/retrieve protocol field, and request content;

a scan module that receives the user request for content and identifies is capable of identifying the request as a request for content by scanning the request content and the request/ retrieve protocol field;

a proxy module that modifies the request for content to be so that it is redirected to a proxy server;

a network that routes the request for content to the proxy server; and

the proxy server that receives the request, forwards the request to the target server, and receives a response from the target server.

2.   (Currently Amended)   The system of claim 1 wherein the proxy server identifies the computer virus undesirable content in the response and processes the response according to defined parameters.

3.   (Currently Amended)   The system of claim 2, wherein the proxy server sends at least a portion of the response to the user, the portion of the response not including the computer virus undesirable content.

4.   (Currently amended)   The system of claim 2, wherein the proxy server sends a notification message back to the user, the notification message containing data related to the computer virus undesirable content.

2

5.   (Original)   The system of claim 1, further comprising:

a user preference module that receives user-defined parameters utilized by the proxy server when processing the response.

6.   (Original)   The system of claim 1, wherein the proxy module redirects the request to the proxy server by modifying the request.

7.   (Original)   The system of claim 6, wherein the proxy module modifies the request by adding a redirection destination header to the request.

8.   (Currently amended)   The system of claim 1, wherein the proxy server further quarantines the computer virus ~~undesirable content~~.

9.   (Cancelled)

10.   (Original)   The system of claim 1, wherein the defined parameters are proxy server default parameters.

11.   (Original)   The system of claim 1, wherein the defined parameters are user-defined parameters.

12.   (Original)   The system of claim 1, wherein the defined parameters are a combination of user-defined parameters and proxy server default parameters.

3

13. (Original)   The system of claim 1, wherein the scan module and the proxy module are located in a network gateway device.

14. (Original)   The system of claim 5, wherein the scan module and the proxy module are located in a network gateway device.

15. (Original)   The system of claim 1, wherein the network gateway device further comprises a firewall and a router.

4

16.   (Currently Amended)   A method for identifying <u>a computer virus</u> ~~undesirable content~~ in responses sent in reply to a user request for content, the method comprising:

receiving input from a user including at least one request for content addressed to a target server<u>, the request having a destination header, a request/retrieve protocol field, and a request content</u>;

identifying the request for content by scanning ~~the~~ <u>only the</u> request <u>content</u> ~~for content~~ <u>and the request/retrieve protocol field</u>;

redirecting the request for content to a proxy server;

receiving the request for content at the proxy server;

sending the request for content from the proxy server to the target server for generation of a response;

receiving the response from the target server at the proxy server;

scanning the response for <u>a computer virus</u> ~~undesirable content~~; and

processing the response according to defined parameters.

17.   (Currently amended)   The method of claim 16, further comprising:

identifying <u>the computer virus</u> ~~undesirable content~~ in the response;

modifying the response to remove the <u>computer virus</u> ~~undesirable content~~; and

sending the modified response from the proxy server to the user.

18.   (Cancelled)

19.   (Original)   The method of claim 16, wherein request for content is redirected to the proxy server by modifying the request.

20.   (Original)   The method of claim 19, wherein the request for content is modified by adding a redirection destination header to the request.

21.   (Original)   The method of claim 16, wherein the request for content is redirected to the proxy server by establishing a session with the proxy server.

5

22.   (Original)   The method of claim 16, further comprising:
receiving input of at least one user-defined parameter for use by the proxy server in processing the computer virus ~~undesirable content~~.

23.   (Original)   The method of claim 22, wherein the user-defined parameter is input using a browser application.

24.   (Previously Amended)   The method of claim 22, wherein the user-defined parameter is sent to the proxy server by modifying the request for content.

25.   (Original)   The method of claim 22, wherein the user-defined parameter is sent to the proxy server during a session established with the proxy server.

Claims 26-27 (Cancelled)

6